AUDITOR-GENERAL'S REPORT
PERFORMANCE AUDIT

Electronic Information Security

The Legislative Assembly
Parliament House
SYDNEY NSW 2000

The Legislative Council
Parliament House
SYDNEY NSW 2000

In accordance with section 38E of the *Public Finance and Audit Act 1983*, I present a report titled **Electronic Information Security.**

Pete Achterstraat

Peter Achterstraat
Auditor-General

Sydney
October 2010

State Library of New South Wales cataloguing-in publication data

New South Wales. Audit Office

Electronic information security / [The Audit Office of New South Wales]. (Performance audit).

978 1921252 457

1. Electronic data processing departments – New South Wales – Auditing. 2. Electronic data processing departments – Security measures – New South Wales – Auditing. 3. Computer security – New South Wales – Auditing. 4. Information storage and retrieval systems – Security measures – New South Wales – Auditing.
I. Title: Electronic information security. II. Title: NSW Auditor-General's report : performance audit : electronic information security. III. Series: Performance audit (New South Wales. Audit Office).

352.379243909944

The Audit Office does not accept responsibility for loss or damage suffered by any person acting on or refraining from action as a result of any of this material.

Contents

Executive summary

Background

The public sector legitimately gathers and uses personal information about citizens, and shares it within and outside government. But personal information can be misused with potentially serious consequences. If the wrong people get access to sensitive personal information an individual can suffer financial loss or damage to their credit rating, have their medical records compromised, or suffer from threats and harassment.

The people of NSW have every right to expect their and their families' private details are secure regardless of which government agency holds it. The Government's current policy on *Security of Electronic Information* acknowledges its duty to safeguard its large information holdings and to provide credible assurance that it is doing so. Under the policy, agencies were to establish and maintain an Information Security Management System (ISMS) that complies with the international standard and covers all electronic information. They were to get and keep the main parts of their ISMS, including the parts that hold sensitive private information, certified to that standard. And the Government Chief Information Office (GCIO) was to survey agencies each year and report to Cabinet.

Our audit assesses the extent to which the Government can provide assurance that it is safeguarding its holdings of sensitive personal information. The audit does this by examining how well the Government's policy has been implemented.

Audit conclusion

The Government is not able to provide assurance that it is safeguarding its holdings of sensitive personal information because its policy has not been properly implemented. This is likely to remain the case until there are clear, mandatory, minimum standards that agencies sign up to, and scrutiny of performance against these standards is strengthened.

Supporting findings

The Government cannot say with any certainty whether agencies have implemented its policy. As a result, the Government does not know how well agencies are securing sensitive personal information.

Progress toward compliance and certification has not been effectively monitored. There is no centrally held, validated information on which agencies are certified to the standard, whether certification actually encompasses sensitive personal information, or even whether agencies comply with the standard but are yet to be certified. That information which does exist suggests at least two thirds of agencies have not complied with the Government's policy.

This is not a new problem. The Government has been issuing edicts about electronic information security for a decade. In 2001, agencies were directed to develop and implement information security policies and have their IT systems certified to the security standard. In 2002, agencies were to report their progress each quarter. In 2004 agencies were told not all had complied, and were directed to adopt an implementation plan by 31 December 2004, with initial certification to be complete by 30 September 2005 and full certification by 30 June 2006.

The current policy followed in 2007. Agencies were again told to get certified to the international standard. But there was no deadline, no effective monitoring, and no consequences if they didn't.

There has been an absence of clear direction and strong leadership to ensure that people's private details are held securely by all government agencies. No one agency has the authority to lead and oversight electronic information security across the NSW public sector and the teeth to make agencies comply.

A fundamental re-think about electronic information security is needed. Government needs to reform the overall arrangements within which agencies manage information security. If anything, IT security is going to get harder not easier. Technological change is speeding up. The level and sophistication of external threats is increasing. And to improve services efficiently, public sector agencies will need to make more use of the personal data they have and share more data with others.

Current initiatives to rationalise, consolidate and standardise Information and Communication Technology (ICT) systems and infrastructure across the NSW Government present an opportunity to improve electronic information security. As these initiatives are implemented, it should become easier to agree upon and implement common standards and approaches, and to hold agencies accountable for meeting them. But aggregating information and consolidating systems may also increase the risk and consequences of unauthorised access to electronic information. This provides an even stronger imperative to ensure electronic information is adequately protected.

A process to develop a new Government ICT strategy and to review ICT governance arrangements across the sector is underway. It is pleasing that this process includes IT security within its scope, and will cover key issues such as standard-setting, monitoring and accountability. It is important that a new ICT strategy with a strong focus on IT security, and improved IT security governance arrangements, are implemented quickly.

Other jurisdictions are also wrestling with how best to ensure electronic information is adequately safeguarded by individual agencies. Our audit identified some common themes in these jurisdictions around improving and strengthening governance and leadership of electronic information security at the centre of government, in particular:

- establishing core minimum standards and mandatory requirements
- strengthening accountability mechanisms
- enhancing scrutiny and transparency of performance.

Our recommendations reflect these themes.

Recommendations

1. The Department of Premier and Cabinet should, on behalf of the NSW Government, publish a new Information and Communication Technology Strategy and establish new electronic information security governance arrangements by June 2011, and ensure that:

Establishing minimum standards and mandatory requirements

1.1. minimum standards, policies, and rules are established with which all agencies must comply, while recognising that individual agencies need to assess their own risk and may need to put in place a higher level of protection

1.2. information security is built into all public sector ICT systems from design through to implementation and disposal

1.3. all ICT products, services and assets adopted by agencies include common standards for information security and, in time, a common and secure infrastructure is used across the public sector

1.4. the processes by which agencies understand and manage their information risks are standardised

1.5. there is one central mechanism for establishing information assurance priorities, sharing risk information across agencies, and sharing best practice

Strengthening accountability

1.6. existing lines of accountability through Directors General and Chief Executive Officers are used to improve information handling, with them signing off on the adequacy of security systems, and information security to be included in their performance agreements

1.7. mandatory training is provided to those with access to sensitive personal information or involved in managing it

1.8. action is taken to make clear that any failure to apply protective measures is a serious matter which could lead to disciplinary action

1.9. professional certification is required for staff or contractors working in roles with technical information security content

Enhancing scrutiny

1.10. visibility of performance is increased, with agencies publishing material in their annual reports, and report to Parliament annually on information security across government

1.11. there is truly independent monitoring of compliance, through audit and technical testing to a defined standard

1.12. agencies report breaches or near misses to an independent organisation responsible for capturing incidents, ensuring investigations are conducted, and lessons are learned.

Response from the Department of Premier and Cabinet

Thank you for the opportunity to respond to your performance audit conducted on whole of Government electronic information security.

The Audit and its findings are both a relevant and timely contribution to the current initiatives and actions already being taken involving the review and revision of the Government's Information and Communication Technology (ICT) policy and forward strategy.

There is no question about the importance of good information security management to the NSW Government, and that there are significant potential risks to be managed, and significant potential costs from information security breaches.

It should be noted that the performance audit has not identified any systemic information security problems within the NSW Government. There is nevertheless the need to properly manage information security risks, and consider future risks and possible problems.

To this end, the existing Government policy on the security of electronic information as provided for in Ministerial Memorandum M2007-04 is now being reconsidered. This includes specifically the appropriateness of the currently mandated requirements for compliance certification. As the Audit notes there are opportunities to achieve greater consistency in implementation throughout the sector.

The Government already has in place a range of mechanisms directed toward the identification and management of information security risks. This includes legislation governing privacy, corruption and financial and records management, as well as NSW Treasury requirements in relation to audit, risk and asset management, procurement, financial management and annual reporting.

Notwithstanding these requirements, the Audit recommends establishing minimum standards and requirements for consistent processes to manage and information assurance risks, as well as strengthening accountability through improved scrutiny and transparency. These initiatives are supported, subject to the outcome of the reforms currently under consideration by Government.

It is pleasing that the Audit has reported that a number of the current key initiatives being implemented within the NSW public sector including the recent agency amalgamations, corporate and shared service reforms and current high level review of ICT strategy and governance are conducive to consolidated whole of government effort and the opportunity for better security of electronic information.

The need to maintain the integrity of information security outcomes is not in dispute, the need to mandate certification requirements remains a contestable strategy. It may be preferable to require agencies to implement information security management systems consistent with international industry standards.

All agencies are required to comply with the Government's Internal Audit and Risk Management Policy for the NSW Public Sector. The Treasury Policy provides a general framework for applying and auditing risk management – Treasury Circular TC 09/08 and Treasury Policy & Guidelines Paper TPP09-5.

The findings of the performance audit and recommendations arising will be referred for consideration in the current Government review of ICT Strategy.

(signed)

Brendan O'Reilly
Director General

Dated 8 October 2010

Key findings

1. Why is electronic information security important?

The digital age

We now live in a digital world. It has changed the way we socialise, communicate, do business and entertain ourselves. Government has not been immune to the digital revolution. The way government works these days is fundamentally different to days gone by. Much sensitive private data is now collected and stored electronically such as:

- details of relationships and family members
- bank accounts, credit card details, salary and financial details
- professional memberships and associations
- driver's licence and other identification information
- medical information
- police records and criminal convictions.

The NSW public sector is also firmly entrenched in the use of internet technologies. These enable better, cheaper and timelier information-based services to the public, and improved collaboration within and between agencies. A good example of this is the Roads and Traffic Authority's myRTA site.

Exhibit 1: myRTA , an example of on-line service delivery

Motor Registry
myRTA.com
Ready when you are
Renewing your rego, changing your address and booking a test are just a few of the things you can do at myRTA.com

Source: http://www.rta.nsw.gov.au/myrta/, August 2010

A 2007 ICAC survey of NSW agencies verified the pervasiveness of digital and internet technologies. It found 80 per cent of NSW public sector organisations can remotely access their IT systems, and 49 percent of organisations have shared services with other organisations or accessed the confidential electronic services of other organisations.

The scale and pervasiveness of information technology is further illustrated in the following data from a recent NSW Treasury review of ICT across government in 2008-09. The review covered general government agencies and non-commercial public trading enterprises representing approximately 95 per cent of the Governments total ICT expenditure. These agencies:

- spent $2 billion on ICT, representing four per cent of total spending
- employed 5,700 ICT staff, representing 2 per cent of total staffing
- had 11,600 computer servers, 298,000 desktop computers, and 69,000 laptops
- had 51,000 terabytes of data storage space.

Changed risks and consequences

The improvements to efficiency and effectiveness associated with digital technologies come at a price, however. Risks change and increase.

Exhibit 2: Trends in global business practices

Since the late 1990s, trends in global business practice have been towards online self-service and collaboration between agencies to cut the costs and inconvenience of duplication. The NSW public sector has been no different. These have many benefits but also require a fresh assessment of risk. In order for the self-service model to succeed certain confidential information of clients must be available to the systems that operate over the internet. Similarly, collaboration through data sharing means that information (some of it confidential) is being transmitted via the internet. Even where confidential data is not being transmitted over the internet by an agency, internet gateways usually exist both in and out of that agency.

Source: Audit Office research 2010

In the paper-based world information about individuals was widely dispersed, and to get at it a wrongdoer had to get to the physical file. Nowadays they could potentially sit at their computer anywhere in the world and get lots of sensitive information about lots of people.

The internet is a global phenomenon and people on the other side of the world can connect to computers on this side. The underlying technology in every country is more or less the same and is probably made by the same set of global manufacturers. Likewise, the software used is the same. The result is that with appropriate access, an experienced user can navigate unknown networks with almost the same ease as they can familiar networks. No longer does information theft require physical access to certain premises. This means that the personal risk associated with trying to gain such physical access has vanished, and convenience for the perpetrator has increased.

These days information can be easily duplicated and transported from a site using USB drives, CDs, a mobile computer or electronically using email or file transfer protocols. This means that confidential data can more easily be moved to a less secure environment. The ease and convenience of transfer also means that besides deliberate acts of theft, data can more easily be incorrectly dispersed or lost.

Personal information can be misused with potentially serious consequences. If the wrong people get access to sensitive personal information, an individual can suffer financial loss or damage to their credit rating, have their medical records compromised, or suffer from threats and harassment.

Exhibit 3: Hypothetical examples of consequences of security breaches

Consequences of IT security breaches could include:

- a criminal gets financial information about a person and empties their bank accounts
- a paedophile deletes their criminal record and attains a job working with children
- a person's medical record is changed and they are given the wrong medicine
- a person is bashed because a violent person finds out who 'dobbed them in' for hitting a child.

Source: Audit Office Research 2010

There are media reports of data theft and loss, and of people being hurt, somewhere in the world nearly every day.

To illustrate, the US Federal Trade Commission estimates that as many as 10 million Americans have their identities stolen each year. While most of these may not be attributed to data stolen from government data repositories, the Commission does describe the impact of identity theft:

> "People whose identities have been stolen can spend hundreds of dollars and dozens of hours cleaning up the mess thieves have made of their good name and credit record. Consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. They may even be arrested for crimes they did not commit. The potential for damage, loss, and stress is considerable."

In June this year, the Audit Office's own security measures blocked 1,667 emails that contained malicious software designed to infiltrate our systems and steal information. The following exhibit provides some relevant examples of electronic information security breaches.

Exhibit 4: Examples of electronic information security breaches

In the United States in 2006, a laptop containing the personal data of 26.5 million military veterans and active-duty personnel was stolen from an employee's home.

In 2009, the Jobs NSW website – its major recruitment tool - was hacked. E-mail addresses of job applicants were stolen, and the applicants were subsequently spammed by the hackers. The hackers used a flaw in the system to penetrate its security. The site was down for many weeks.

In late 2009, RailCorp networks were infected by the Conficker virus. Conficker disables many security services on the computers it infects with the intent of permitting hackers remote access to both the computers and the network where they reside. Any data held on infected computers is therefore vulnerable to theft or modification by hackers

Earlier this year, the NSW Government's Transport Blueprint was leaked when the NSW Department of Transport's contractor accidentally removed a layer of security over it.

Source: Audit Office research 2010

There could be more such incidents. Unless breaches are exposed in the media knowledge of them tends to remain limited. Identifying both poorly and strongly defended systems in any form of public forum is likely to make that system a target. Keeping quiet makes it harder for a victim to identify how a wrongdoer got hold of their private information, and to hold the organisation accountable for its lax security. And in some cases, an organisation may never know it has been compromised, particularly if it is not that good at IT security.

If anything, threats to information assets are increasing. A survey of around 4,000 businesses by the Australian Institute of Criminology found 14 percent of businesses during the 2007 financial year suffered unauthorised use, damage, attack or theft of information. A 2009 Ernst and Young survey of around 1,900 senior executives in more than 60 countries reported a 25 percent increase in internal attacks, and a 41 percent increase in external attacks over the previous year.

Also, without assurance of consistently high security standards, agencies with high quality security are likely to be unwilling to share information with those with lower security standards, putting at risk the type of inter-agency information exchange promoted by the government's ICT Strategy.

Exhibit 5: The Government's Information and Communication Technology Strategy promotes data sharing

The NSW Government's Information and Communication Technology Strategy, *People First*, advocates "the flow of information and knowledge between NSW Government agencies, government workers, and the public", with the argument that "having better access to the right information is critical to improving the delivery of services to the public and the public's experience in dealing with government."

Source: People First. NSW GCIO

2. Is electronic information adequately safeguarded?

Key finding

The Government is not able to provide assurance that agencies are adequately safeguarding the sensitive private information they hold. The GCIO does not have current and reliable information on how well individual agencies are safeguarding private information. That information which is available suggests most agencies have not complied with the Government's policy. Government needs to reform the overall arrangements within which agencies manage information security.

The Government's current policy

The Government's current policy objective is outlined in Ministerial Memorandum 2007-04 *Security of Electronic Information* issued by the then Premier in 2007:

> "The Government has a duty to safeguard its large information holdings and must provide credible assurance that it is doing so."

M2007-04 also outlines the means by which the policy was to be achieved. It says that all agencies that process, hold or use electronic information or data were to, as soon as possible:

- establish and maintain an agency wide Information Security Management System that complies with the international standard (ISO/IOC 27001) and covers all electronic information; and
- gain and maintain certified compliance to the standard (ISO/IOC 27001) of the main part(s) of their Information Security Management System by an accredited certifier.

Exhibit 6: The international standard - ISO/IEC 27001

ISO/IEC 27001 is the auditable international standard which defines the requirements for an Information Security Management System (ISMS).

The standard is designed to ensure the selection of adequate and proportionate security controls. It adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the ISMS.

This helps organisations protect their information assets and give confidence to interested parties. Certifying against ISO/IEC 27001:

- provides independent assurance of the adequacy of internal controls and that risks are identified, assessed and managed
- helps organisations to continually monitor performance and improve
- demonstrates an organisations commitment to the security of its information.

Source:http://www.bsigroup.com.au/en-au/Assessment-and-Certification-services/Management-systems/Standards-and-schemes/ISOIEC-27001/

Further, the memorandum says:

- certification is to cover information about identifiable members of the public
- the GCIO is to survey security status annually, and report the result to Cabinet.

The policy is not being implemented properly

We found that the GCIO conducted an online survey in late 2007.

Exhibit 7: Key results of 2007 GCIO survey

Ninety-seven agencies responded to the 2007 GCIO survey. Of these agencies:

- 26 had part of their ISMS certified to the national standard
- 20 planned to get part of their ISMS certified in 2008
- 6 more planned to get part of their ISMS certified by 2010.

In 2007, one more agency was certified (that is, 27 in total) but did not complete the GCIO survey.

Source: GCIO 2009

We also found that GCIO:

- did not report the results to Cabinet
- has not conducted any further surveys, and has no plans to do so.

The certifying bodies publish registers of certified organisations on-line. These show that about one-third of NSW agencies have at least part of their Information Security Management System currently certified to the international standard.

However, GCIO advises that it cannot:

- attest to the accuracy of this information
- say whether all private information held in these agencies is covered
- advise on the progress made in the remaining two-thirds of agencies towards compliance and certification.

This has been a problem for a decade

This is not a new problem. The government has been issuing edicts to agencies about electronic information security for a decade with little impact.

Exhibit 8: Prior edicts on information sharing

Department of Premier and Cabinet Circular 2001-46 directed all NSW agencies to develop and implement information security policies and have their IT systems certified to the existing security standard by 2002.

Ministerial Memorandum 2001-14 directed all NSW agencies to report their progress on the above each quarter to the end of 2002.

Department of Premier and Cabinet Circular 2004-06 reminded agencies of the 2001 directive, and acknowledged that not all agencies had complied. It required agencies to adopt an implementation plan by 31 December 2004, with initial certification to be complete by 30 September 2005, and full certification by 30 June 2006.

Source: Department of Premier and Cabinet, 2010

The 2007 policy told agencies to get certified to the international standard, but there was no deadline, no effective monitoring, and no consequences if they didn't. The Department of Premier and Cabinet and the Department of Services, Technology and Administration (DSTA) acknowledge that the Government's electronic information security policy could be implemented more consistently, and that benefits will result from:

- a more standardised approach to how agencies understand and manage their information risks
- a clear whole-of-government picture of risk.

DSTA says that the onus for implementation of the Government's electronic information security policies rests with agencies and departments as there is no central regulation of compliance with the policy.

Fundamental change is needed

There is clearly a need to change the means by which the Government's policy objective is being implemented. Otherwise, the Government will continue to be unable to assure the people of NSW that its agencies are safeguarding their private information. The Department of Premier and Cabinet and the Department of Services, Technology and Administration (DSTA) support having appropriate information security arrangements.

If anything, IT security is going to get harder not easier. Technological change is speeding up. The level and sophistication of external threats is increasing. And to improve services efficiently, public sector agencies will need to make more use of the personal data they have and share more data with others.

DSTA advises that a significant improvement in IT security will require:

- clearer identification of roles and responsibilities in relation to the management of information security risk
- a clear policy mandate to develop and implement whole-of-government information security policy
- appropriate resourcing to develop and monitor the implementation of consistent information security practices across the sector.

Other initiatives present an opportunity to reform IT security

The Government is re-thinking how ICT generally should be managed and delivered. To date, this has occurred in a fragmented way across the sector, with a high degree of local decision making leading to significant variation across the NSW Government. The Government's Corporate and Shared Services Blueprint (May 2010) describes the current situation:

> Corporate and Shared Services functions (including ICT) are currently provided in a fragmented way across the sector, with some provided internally and some externally to departments. There is a significant variation across the clusters in the maturity of expectations, understanding, delivery and usage of these types of services.

Several current and recent reform initiatives are designed to aggregate, rationalise and standardise ICT systems and infrastructure, and generate greater consistency in approach across the public sector. These reform initiatives include the:

- amalgamation of 160 agencies into 13 clusters, each with a Principal Department, effective from 1 July 2009
- Corporate and Shared Services Strategy to develop 13 corporate service providers and six shared service providers so as to achieve industry best practices and better support frontline services
- strategic review of whole-of-government ICT expenditure which is aiming to make sustainable improvements in the efficiency of the Government's ICT expenditure, leading to ongoing cost savings from 2010-11 onwards
- Data Centre program to aggregate data storage.

More detail on these initiatives can be found at appendix 2.

Aggregating electronic information and consolidating ICT systems present an opportunity to reform security, but also increase the risk and consequences of unauthorised access to information. This provides an even stronger imperative to ensure electronic information is adequately protected.

The current whole-of-government ICT Strategy, PeopleFirst (led by DSTA), concluded on 30 June 2010. Recognising this, and the abovementioned reforms, a process to develop a new Government ICT strategy and to review ICT governance arrangements across the NSW Government is underway. The first stage of this project is a high level review to outline the broad definition, scope and key issues to be addressed in the development of the new ICT Strategy. The Review will include an assessment of options for future ICT governance and delivery arrangements to ensure effective implementation of the new Strategy and public sector reform programs.

Exhibit 9: High level review - future ICT strategy and governance

The Review will cover a range of issues including:

- the respective roles, responsibilities, and accountabilities of central agencies, DSTA and departmental CIOs in reviewing, developing and implementing whole-of-government ICT strategies, frameworks, policies, standards, etc
- ICT governance and ICT delivery and implementation arrangements, including policy setting, strategy development, standards setting, resource prioritisation, and technology and capability development
- organisational arrangements to support optimal whole-of-government ICT governance and ICT delivery arrangements, including indicative organisational structures and functions.

The terms-of-reference indicate that the security of electronic information will be an important part of the Review, and that it will have regard to better practice approaches elsewhere.

The Review is scheduled to report to the Directors General of the DP&C and DSTA, and the Secretary of NSW Treasury, by the end of October 2010. It will include a timetable for publication of the new Strategy and establishment of new governance arrangements.

Source: Department of Premier and Cabinet, 2010

Recommendation

The Department of Premier and Cabinet should develop and publish by June 2011:

- a new Government ICT strategy with a strong focus on IT security
- improved whole-of-government IT security governance arrangements.

NSW reforms should take account of developments elsewhere

Other jurisdictions are also wrestling with how best to ensure electronic information is adequately safeguarded. Our research identified that steps are being taken in several jurisdictions to strengthen governance and leadership of electronic information security at the centre of government. These fall into three key themes:

- establishing core minimum standards and mandatory requirements
- strengthening accountability mechanisms, and promoting a culture that values, protects and uses data properly
- enhancing scrutiny and transparency of performance, to drive compliance and ensure lessons are learned.

Minimum standards and mandatory requirements

The UK government is setting clear common standards and procedures to enhance consistency of protection of electronic information across government. The guiding principle is that the minimum protections should be in place and effective, no matter how information is held and processed for UK Government purposes.

For example, the UK Government is introducing obligatory use of protective measures (such as encryption and penetration testing) and controls (for example on use of mobile devices or on access to records). These will protect all personal data, while recognising that some data require a greater degree of protection than others. Individual agencies, however, assess their own risk and often put in place a higher level of protection. The Cabinet Office is responsible for reviewing and updating the standards in the future to accommodate lessons learned and new developments.

In its recent (2010) ICT policy, the UK Government also indicated that information security will be built into every IT system, from requirements capture through design, implementation and disposal. The aim is to facilitate data sharing and make it easier to join up public services. The UK is also seeking to standardise and enhance the processes by which Departments understand and manage their information risk.

Victoria has also recently issued a number of minimum standards.

Exhibit 10: Victorian information security standards

Data classification and management - This Standard describes the requirement for each department and agency to assess and manage the exposure risk of confidential information under its control, via a three part process.

Penetration testing - This standard describes the minimum requirement for Victorian Government departments and agencies to conduct independent penetration testing on their information systems and infrastructure to identify vulnerabilities and weaknesses in security controls.

Use of portable storage devices - This standard provides an overview of the risks associated with the use of these devices, the associated controls and risk mitigation measures that must be implemented, and the rationale for the controls.

Evidence of identity: This standard describes the requirements for evidence of identity for Victorian Government staff and details the documentation required for the process.

Mechanism strength: This standard describes the requirements for selecting a suitable online authentication mechanism (i.e. credential) for staff accessing information in Victorian Government systems.

Passwords: This standard describes the characteristics and management requirements for passwords as online authentication mechanisms (i.e. credentials) for staff accessing information in Victorian Government systems.

Two-factor credentials: This standard describes the application of two-factor credentials for the online authentication of staff accessing information in Victorian Government systems. It directs the government-supplied source for credentials.

Source: Victorian Department of Treasury and Finance, 2010

Recommendations

The Department of Premier and Cabinet should ensure:

- minimum standards, policies, and rules are established with which all agencies must comply, while recognising that individual agencies need to assess their own risk and may need to put in place a higher level of protection
- information security is built into in all public sector ICT systems from design through to implementation and disposal
- all ICT products, services and assets adopted by agencies include common standards for information security, and in time a common and secure infrastructure is used across the public sector
- the processes by which agencies understand and manage their information risks are standardised
- there is one central mechanism for establishing information assurance priorities, sharing risk information across agencies, and sharing best practice.

Strengthening accountability

A common approach to introduce stronger accountability mechanisms is to make the heads of agencies clearly responsible for meeting minimum standards and adequately protecting sensitive personal information.

To illustrate, the UK Government is using the existing line of accountability through Accounting Officers to Parliament as a way to improve information handling; recognising that the individual Department or agency is best placed to understand and address risks to their information, including personal data.

The UK government is also seeking to ensure that civil service culture supports the proper use of information. Strategies include:

- mandatory training for those with access to protected personal information or involved in managing it, with more than 300,000 civil servants dealing with personal data undertaking mandatory annual training
- new action to make clear that any failure to apply protective measures is a serious matter potentially leading to dismissal, including new sanctions under the Data Protection Act for the most serious breaches of its principles
- data security roles within departments have been standardised and enhanced to ensure clear lines of responsibility.

Recommendations

The Department of Premier and Cabinet should ensure:

- existing lines of accountability through Directors General and Chief Executive Officers are used to improve information handling, with them signing off on the adequacy of security systems, and information security to be included in their performance agreements
- mandatory training is provided to those with access to sensitive personal information or involved in managing it
- action is taken to make clear that any failure to apply protective measures is a serious matter which could lead to disciplinary action
- professional certification is required for staff or contractors working in roles with technical information security content

Enhanced scrutiny

Since a critical performance audit in 2009, the Victorian Department of Treasury and Finance has enhanced scrutiny of agency compliance with electronic information security policies and standards.

Its 2010 Reporting calendar for information security, including access management, illustrates their approach.

Exhibit 11: Victoria's 2010 Reporting calendar - Information security

Due	Standard	Requirement	Template
June	Identity and access management	Plan for compliance with Identity Access Management standards	WoVG Security reporting
June	Information security	Planned program of work for compliance with Penetration Testing standard	WoVG Security reporting
June	Information security	Plan for compliance with Portable Storage Devices standard	WoVG Security reporting
Nov	Identity and access management	Report progress against plan of compliance with Identity Access Management standards	WoVG Security reporting
Nov	Information security	Report progress against plan of compliance with Management Framework standard	Compliance report information security
Nov	Information security	Report security-classified systems annually	System operational description information security
Nov	Information security	Reporting of all penetration testing annually	Penetration testing compliance reporting
Nov	Information security	Report progress against plan of compliance for Portable Storage Devices annually	WoVG Security reporting template

Source: Victorian Department of Treasury and Finance, 2010

Queensland has a system of self assessment, reporting and auditing.

Exhibit 12: Queensland Information Security Standards compliance regime

Queensland public sector agencies are required to meet Information Standard 18 (IS18). The authority for IS18 comes from a Cabinet mandate. IS18 is closely aligned to ISO27001 but is specifically tailored to the needs of the Queensland Government. An example of this is the Queensland Government Information Security Classification Framework.

Agencies self-assess compliance against the mandatory requirements of IS18 annually and provide the results to the Government Chief Information Officer and an Information Security Committee comprising agency CIO's or their proxies. Non-compliance may also picked up via audits against IS18 by the Queensland Audit Office.

Source: Qld ICT Policy & Coordination Office, 2010

The UK Government claims that at the centre of government, the governance of information assurance has been improved and strengthened with enhanced oversight now in place at ministerial and senior official levels. It has adopted a number of strategies to increase scrutiny of performance, to build confidence, and ensure that lessons are learned and shared:

- departments report annually on their performance in handling information risk
- the Information Commissioner conducts spot checks of agencies
- the National Audit Office audits the Statement on Internal Control, which includes controls over personal data
- Cabinet Office reports annually to Parliament on the issue as a whole.

Recommendations

The Department of Premier and Cabinet should ensure:

- visibility of performance is increased, with agencies publishing material in their annual reports, and report to Parliament annually on information security across government
- there is truly independent monitoring of compliance, through audit and technical testing to a defined standard
- agencies report breaches or near misses to an independent organisation responsible for capturing incidents, ensuring investigations are conducted, and lessons are learned.

Appendices

Appendix 1 About the audit

Audit objective

Our audit assessed the extent to which the Government can provide credible assurance that it is safeguarding its holdings of sensitive personal information.

Audit criteria

Our criterion (the ‘what should be’) for the audit was that the Government should be able to show that those systems which hold personal information are certified to comply with the international Information Security Management Systems standard.

The criterion was derived from the Government’s policy on Security of Electronic Information described in Ministerial Memorandum 2007-04. The objective of the policy is to allow the Government to provide credible assurance that it is safeguarding its large information holdings.

Under the policy, agencies were to establish and maintain an Information Security Management System (ISMS) that complies with the international standard and covers all electronic information. They were to get and keep the main parts of their ISMS, including the parts that hold sensitive private information, certified to that standard. And the Government Chief Information Office was to survey agencies each year and report to Cabinet.

Our audit criteria are always discussed and, wherever possible, agreed with those we are auditing.

Originally, we planned to have two additional criteria, that is:

- personal information held on selected databases is adequately protected from unauthorised access.
- unencrypted sensitive personal information is rarely emailed outside the selected agencies.

During the audit, we decided to include these in a separate report at a later date as a Special Review under s52(3) of the Public Finance and Audit Act.

Audit scope

The audit focused on compliance with the Government’s policy at the time of the audit. It did not seek to obtain information from all government agencies on the basis that the policy required GCIO to collect such information annually.

Audit approach

The audit team acquired subject matter expertise by:

- examining relevant policy documents and progress reports
- interviewing relevant staff of DSTA, DP&C and others
- researching publicly available information on approaches in other jurisdictions
- retaining Mr Christopher Grant, Ernst and Young, as a subject-matter expert.

Audit selection

We use a strategic approach to selecting performance audits which balances our performance audit program to reflect issues of interest to Parliament and the community. Details of our approach to selecting topics and our forward program are available on our website.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Standard on Assurance Engagements ASAE3500 on performance engagements and to reflect current thinking on performance auditing practices.

Audits are produced under the Office's quality control policies and practices, including a quality management system certified to International Standard ISO 9001. Our processes have also been designed to comply with the *Public Finance and Audit Act 1983*.

Acknowledgement

We gratefully acknowledge the co-operation and assistance provided by The Department of Premier and Cabinet, Department of Services, Technology and Administration, and NSW Treasury.

Audit team

Our team leader for this performance audit was Rod Longford, who was assisted by Greg Long. Sean Crumlin provided direction and quality assurance.

Audit report cost

Including staff costs, printing costs and overheads the estimated cost of this audit report is $122,500. This excludes the cost of work which will be reported separately as a Special Review.

Appendix 2 Public sector reform initiatives relevant to Electronic Information Security

Agency amalgamations

In mid 2009, the NSW Government announced major changes to the structure of Government, through amalgamating agencies into 13 clusters. Clusters contain a Principal Department and usually also include agencies and a range of other bodies, such as tribunals or statutory bodies. The aim is to deliver more integrated services, stronger customer focus, and more efficient provision of Corporate and Shared Services.

Source: Department of Premier and Cabinet, 2010

Corporate and Shared Services Strategy

In May 2010, the Corporate and Shared Services Blueprint was released. It aims to provide a whole-of-government framework that will enable Principal Departments to achieve benefits from the consolidation of Corporate and Shared Services. The objectives of the Blueprint are to:

- provide sector wide consistency and standardisation within the areas of Corporate and Shared Services while acknowledging the uniqueness and complexity of individual departments and the services they provide
- establish parameters for departments to make decisions that are aligned to whole of government objectives
- hardwire key decisions to minimise or prevent loss of potential benefits across Departments.

A key Blueprint principle is standardisation of processes, systems and service levels within clusters and across government – referenced to industry standards and best practices. The longer term aim is for five in-house Shared Services providers and one multi-tenanted provider, all supported by a single ICT Wholesale operator.

Source: Department of Premier and Cabinet, 2010

Data Centre Program

The Data Centre Program aims to establish two fit-for-purpose data centres to house the computer systems and associated components of NSW Government agencies' data centres currently scattered across NSW.

Source: GCIO 2010

Strategic review of ICT expenditure ("ICT Review") across NSW Government Agencies and Public Trading Enterprises

The objective of the ICT Review is to make sustainable improvements in the efficiency of the Government's ICT expenditure, leading to ongoing cost savings from 2010-11 onwards. This must be achieved without impairing service delivery to residents or business.

The ICT Review requires NSW Government Agencies and Public Trading Enterprises to find savings equivalent to five per cent of their baseline ICT expenditure (Phase 1) and an additional 10 per cent (Phase 2) over four years.

Fifty per cent of the cost savings delivered from the ICT Review are to be placed in the centrally held ICT Reinvestment Pool. The ICT Reinvestment Pool will be used to fund investment in strategic efficiency improving ICT capital projects.

Source: NSW Treasury, 2010

Performance Audits by the Audit Office of New South Wales

Performance Auditing

What are performance audits?

Performance audits determine whether an agency is carrying out its activities effectively, and doing so economically and efficiently and in compliance with all relevant laws.

The activities examined by a performance audit may include a government program, all or part of a government agency or consider particular issues which affect the whole public sector. They cannot question the merits of Government policy objectives.

The Auditor-General's mandate to undertake performance audits is set out in the *Public Finance and Audit Act 1983*.

Why do we conduct performance audits?

Performance audits provide independent assurance to Parliament and the public that government funds are being spent efficiently, economically or effectively and in accordance with the law.

Through their recommendations, performance audits seek to improve the efficiency and effectiveness of government agencies so that the community receives value for money from government services.

Performance audits also focus on assisting accountability processes by holding managers to account for agency performance.

Performance audits are selected at the discretion of the Auditor-General who seeks input from Parliamentarians, the public, agencies and Audit Office research.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing. They can take up to nine months to complete, depending on the audit's scope.

During the planning phase the audit team develops an understanding of agency activities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the agency or program activities are assessed. Criteria may be based on best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork the audit team meets with agency management to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with agency management to check that facts presented in the draft report are accurate and that recommendations are practical and appropriate.

A final report is then provided to the CEO for comment. The relevant Minister and the Treasurer are also provided with a copy of the final report. The report tabled in Parliament includes a response from the CEO on the report's conclusion and recommendations. In multiple agency performance audits there may be responses from more than one agency or from a nominated coordinating agency.

Do we check to see if recommendations have been implemented?

Following the tabling of the report in Parliament, agencies are requested to advise the Audit Office on action taken, or proposed, against each of the report's recommendations. It is usual for agency audit committees to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament's Public Accounts Committee (PAC) to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report is tabled. These reports are available on the Parliamentary website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian and international standards.

Internal quality control review of each audit ensures compliance with Australian assurance standards. Periodic review by other Audit Offices tests our activities against best practice. We are also subject to independent audits of our quality management system to maintain certification under ISO 9001.

The PAC is also responsible for overseeing the performance of the Audit Office and conducts a review of our operations every three years. The review's report is tabled in Parliament and available on its website.

Who pays for performance audits?

No fee is charged for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in-progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

Performance Audit Reports

No	Agency or Issues Examined	Title of Performance Audit Report or Publication	Date Tabled in Parliament or Published
207	Whole of Government electronic information security	*Electronic Information Security*	October 2010
206	NSW Health NSW Ambulance Service	*Helicopter Emergency Medical Service Contract*	22 September 2010
205	Department of Environment, Climate Change and Water	*Protecting the Environment: Pollution Incidents*	15 September 2010
204	Corrective Services NSW	*Home Detention*	8 September 2010
203	Australian Museum	*Knowing the Collections*	1 September 2010
202	Industry & Investment NSW Homebush Motor Racing Authority Events NSW	*Government Investment in V8 Supercar Races at Sydney Olympic Park*	23June 2010
201	Department of Premier and Cabinet	*Severance Payments to Special Temporary Employees*	16 June 2010
200	Department of Human Services - Ageing, Disability and Home Care	*Access to Overnight Centre-Based Disability Respite*	5 May 2010
199	Department of Premier and Cabinet NSW Treasury WorkCover NSW	*Injury Management in the NSW Public Sector*	31 March 2010
198	NSW Transport and Infrastructure	*Improving the Performance of Metropolitan Bus Services*	10 March 2010
197	Roads and Traffic Authority of NSW	*Improving Road Safety: School Zones*	25 February 2010
196	NSW Commission for Children and Young People	*Working with Children Check*	24 February 2010
195	NSW Police Force NSW Department of Health	*Managing Forensic Analysis – Fingerprints and DNA*	10 February 2010
194	Department of Premier and Cabinet Department of Services, Technology and Administration NSW Treasury	*Government Advertising*	10 December 2009
193	Roads and Traffic Authority of NSW	*Handback of the M4 Tollway*	27 October 2009
192	Department of Services, Technology and Administration	*Government Licensing Project*	7 October 2009
191	Land and Property Management Authority Maritime Authority of NSW	*Administering Domestic Waterfront Tenancies*	23 September 2009
190	Department of Environment, Climate Change and Water NSW Environmental Trust	*Environmental Grants Administration*	26 August 2009
189	NSW Attorney General's Department NSW Department of Health NSW Police Force	*Helping Aboriginal Defendants through MERIT*	5 August 2009

No	Agency or Issues Examined	Title of Performance Audit Report or Publication	Date Tabled in Parliament or Published
188	NSW Department of Health	*Tackling Cancer with Radiotherapy*	23 June 2009
187	Roads and Traffic Authority of NSW	*Improving Road Safety – Heavy Vehicles*	13 May 2009
186	Grants	*Grants Administration*	6 May 2009
185	Forests NSW	*Sustaining Native Forest Operations*	29 April 2009
184	NSW Police Force	*Managing Injured Police*	10 December 2008
183	Department of Education and Training	*Improving Literacy and Numeracy in NSW Public Schools*	22 October 2008
182	Department of Health	*Delivering Health Care out of Hospitals*	24 September 2008
181	Department of Environment and Climate Change	*Recycling and Reuse of Waste in the NSW Public Sector*	11 June 2008
180	Follow-up of 2003 Performance Audit	*Protecting Our Rivers*	21 May 2008
179	NSW Office of Liquor, Gaming and Racing; NSW Police Force	*Working with Hotels and Clubs to reduce alcohol-related crime*	23 April 2008
178	Greyhound and Harness Racing Regulatory Authority	*Managing the Amalgamation of the Greyhound and Harness Racing Regulatory Authority*	3 April 2008
177	Office of the Director of Public Prosecutions	*Efficiency of the Office of the Director of Public Prosecutions*	26 March 2008
176*	Better Practice Guide	*Implementing Successful Amalgamations*	5 March 2008
175	Department of Commerce Department of Primary Industries	*Managing Departmental Amalgamations*	5 March 2008
174	Department of Education and Training	*Ageing workforce – Teachers*	13 February 2008
173	NSW Police Force	*Police Rostering*	5 December 2007
172	Department of Primary Industries	*Improving Efficiency of Irrigation Water Use on Farms*	21 November 2007
171	Department of Premier and Cabinet Department of Commerce	*Government Advertising*	29 August 2007
170	RailCorp	*Signal Failures on the Metropolitan Rail Network*	15 August 2007
169	NSW Police Force	*Dealing with Household Burglaries*	27 June 2007
168	Ministry of Transport	*Connecting with Public Transport*	6 June 2007

* Better Practice Guides

Performance audits on our website

A list of performance audits tabled or published since March 1997, as well as those currently in progress, can be found on our website www.audit.nsw.gov.au.

If you have any problems accessing these reports, or are seeking older reports, please contact our Office Services Manager on (02) 9275 7116.